



中华人民共和国国家标准

GB/T 37970—2019

软件过程及制品可信度评估

Trustworthiness assessment for software process and artifact

2019-08-30 发布

2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 软件可信度模型	3
4.1 模型概述	3
4.2 软件过程可信原则	4
4.3 软件制品可信原则	7
4.4 软件过程可信证据	7
4.5 软件制品可信证据	11
5 软件可信度等级	17
5.1 软件过程可信度等级	17
5.2 软件制品可信度等级	18
6 软件过程可信度评估	19
6.1 软件过程可信度评估过程	19
6.2 过程证据的可信度评估	19
6.3 可信原则的可信度评估	20
6.4 软件过程的可信度评估	20
7 软件制品可信度评估	20
7.1 软件制品可信度评估过程	20
7.2 制品证据的可信度评估	20
7.3 软件制品的可信度评估	21
附录 A (资料性附录) 可信原则与 CMMI 过程域	22
附录 B (规范性附录) 软件过程证据	24
附录 C (规范性附录) 软件制品证据	39
附录 D (资料性附录) 软件可信度评估示例	52
参考文献	56

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:中国科学院软件研究所、中国电子技术标准化研究院、南京大学、中国科学院科技战略咨询研究院、厦门理工学院、上海计算机软件技术开发中心、重庆邮电大学、北京拓尔思信息技术股份有限公司、罗普特(厦门)科技集团有限公司、北京知道未来信息技术有限公司。

本标准主要起草人:王丹丹、王德鑫、刘增志、赖宜亮、韦庆杰、吴登生、胡芸、冯志超、贺劼、王林章、崔建峰、张旻旻、王青。

引 言

质量形成于过程。软件可信的基本问题是需要有证据证明软件产品能够满足用户的需求,而这些证据散布于软件开发的整个生存周期。所以,软件是否可信不能仅依赖于对最终产品的测试,对软件可信的评估和确认需要软件开发过程中各类相关证据的支持。本标准旨在从软件过程及制品的角度,建立系统化的可信度评估模型,指导软件开发在过程中采集合适的数据,以形成证据,支持证据驱动下的软件可信度评估。

软件可信并非一个新的质量特性,而是对软件的功能性、安全性、可维护性、可靠性等各种质量特性满足需求的程度的测量。受传统行业全面质量管理理论的启发,本标准提出面向过程的方法,通过关注和提高软件开发过程的质量,来提高软件的可信度。CMMI 是被业界广泛采用的软件过程管理框架,目前运行的 CMMI V1.3 包括 22 个过程域,用软件开发过程的知识技术解决软件管理流程,强调改进软件过程能力,提高软件过程的成熟度,从而帮助企业有预期地、稳定地在预算内按时交付满足用户要求的产品。

本着兼容国际流行技术的准则,提出软件过程可信原则覆盖 CMMI V1.3 的 22 个过程域,另外扩充了对可信实体的保障,并通过制品可信原则对软件过程的制品进行了可信增强。形成的软件过程及制品可信证据体系,将软件质量分解到软件开发的各个阶段和过程,有目标地采集过程数据,形成覆盖软件开发全过程的证据链,并最终对交付的软件产品满足预期质量目标的可信度进行评估。

软件过程及制品可信度评估

1 范围

本标准规定了软件过程和制品可信度评估使用的模型、可信等级和评估方法。

本标准适用于指导开发软件产品的组织建立可信的软件过程,并采集数据,积累证据以支持对软件产品质量的信心。同时也适用于第三方评估认证机构建立评估方法,对目标软件产品及其开发组织开展第三方评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 19001—2016 质量管理体系 要求

GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第10部分:系统与软件质量模型

GB/T 25000.23—2019 系统和软件工程 系统与软件质量要求和评价(SQuaRE) 第23部分:系统与软件产品质量测量

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25000.10—2016、GB/T 25000.23—2019 和 GB/T 19001—2016 界定的以及下列术语和定义适用于本文件。

3.1.1

过程 process

为给定目的所执行的步骤序列,例如,软件开发过程。

[GB/T 11457—2006,定义 2.1183]

3.1.2

软件过程 software process

由组织或项目使用的,用以计划、管理、执行、监控和改进其软件相关活动的过程或过程的集合。

[GB/T 11457—2006,定义 2.1512]

3.1.3

软件开发全过程 whole process of software development

软件开发中的需求、设计、编码和测试过程。

注:与 GB/T 11457—2006 中定义的开发过程相比,为便于可信指标的分类,软件开发全过程专指需求、设计、编码和测试四个过程。

3.1.4

制品 artifact

由某一种软件开发过程所使用的或产生的一种信息的物理件。制品的实例有模型、源文件、文字和